(Translation of a notice from the Japanese Patent Office)

Mailing No. 194930
Mailing Date: June 18, 2002

NOTIFICATION OF REASONS FOR REJECTION

Patent Application No.: 2000-261098
Examiner's Notice Date: June 13, 2002
Examiner: Shigenori Aoki
Attorneys on Record: Takehiko Suzuye

This application is rejected on the grounds stated below. Any opinion about the rejection must be filed within 60 days of the mailing date hereof.

REASON

[A] The application fails to satisfy the requirements under the main provision of Section 29 of the Patent Law in the following respects.

REMARKS

· Claims 11 and 25

· Note

An invention considered to be a computing method or plotting method generally utilizes human deductive powers or memory, and does not involve technical means utilizing a law of natural. In principle, such an invention is not judged to satisfy the requirements under Section 29 of the Patent Law.

"An extended key generation method" recited in claims 11 and 25 defines a method for generating an extended key through computing or plotting from an encrypted key generally represented as numerals. Since no device is involved during this process, the above principle can apply by analogy.

Therefore, the invention recited in claims 11 and 25 does not fall under "the invention" described in Section 2 of the Patent Law.

· Claims 12-21 and 26

· Note

Since "a computer readable storage medium" recited in claims 12-21 and 26 does not use any technical means during the process, it is considered that the medium merely stores programs defining artificial arrangement. Therefore, the invention recited in claims 12-21 and 26 simply presents information, and does not fall under "the invention" described in Section 2 of the Patent Law.

REASON

[B] The invention recited in the following claims is unpatentable under Section 29 (2) of the Patent Law, as being such that the invention could easily have been accomplished by a person having ordinary knowledge in the technical field to which such an invention belongs, on the basis of the invention described in the following publications distributed in Japan or a foreign country prior to this application.

REMARKS

· Claims 1, 4 and 5

· Reference 1

· Note

Reference 1 discloses an apparatus comprising a key schedule portion having cascade-connected intermediate key generating circuits, in which each intermediate key generating circuit performs conversion by a predetermined function based on a first key obtained from an input key, and computes an intermediate key based on the result of the conversion and a second key obtained from the input key.

In the apparatus described in Reference 1, key conversion is achieved by a function process. However, the function process is based on a conversion table using a so-called s box. In view of this matter, the apparatus disclosed in Reference 1 has a functional structure essentially the same as that of the invention recited in claim 1 of the present application.

· Claim 2

· References 1 and 2

· Note

Reference 2 discloses a key schedule portion which shifts an input key to the left and inputs it to a next key schedule portion.

Since both References 1 and 2 describes a technique for generating an extended key, it would have been obvious to a person skilled in the art to use the structure disclosed in Reference 2 as the input structure for the next key schedule portion of the apparatus disclosed in Reference 1.

· Claims 9 and 10

· Reference 1

· Note

The apparatus disclosed in Reference 1 uses a plurality of generated intermediate keys as keys of a function process in each round, and performs a mixing process for encrypting a plaintext and decrypting a ciphertext to a plaintext.

· Claims 11, 12, 20, 21, 25 and 26

· Reference 1

· Note

Reference 1 discloses an apparatus comprising a key schedule portion having cascade-connected intermediate key generating circuits, in which

each intermediate key generating circuit performs conversion by a predetermined function based on a first key obtained from an input key, and computes an intermediate key based on the result of the conversion and a second key obtained from the input key.

In the apparatus described in Reference 1, key conversion is achieved by a function process. However, the function process is based on a conversion table using a so-called s box. In view of this matter, the apparatus disclosed in Reference 1 has a functional structure essentially the same as that of the invention recited in claim 1 of the present application. It is commonly used means for a person skilled in the art to store such a method in a storage medium as a program in order to implement it with a computer.

- Claim 13
- References 1 and 2
- Note

Reference 2 discloses a key schedule portion which shifts an input key to the left and inputs it to a next key schedule portion.

Since both References 1 and 2 describes a technique for generating an extended key, it would have been obvious to a person skilled in the art to use the structure disclosed in Reference 2 as the input structure for the next key schedule portion of the apparatus disclosed in Reference 1. It is commonly used means for a person skilled in the art to store such a method in a storage medium as a program in order to implement it with a computer.

References:

1. Akihiro Shimizu and Shoji Miyaguchi, "High-speed Data Encryption

Algorithm FEAL", an anthology D of THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS, Japan, THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS, July 20, 1987, Vol. J70-D, No. 7, pp. 1413-1423

2. Jpn. Pat. Appln. KOKAI Publication No. 10-116029

REASON

[C] The application fails to satisfy the requirements under Section 36 (6) (i) of the Patent Law, on the grounds that the claims are defective in the following respect.

REMARKS

The specification and drawings of the present application disclose a technique for inputting a temporary key generated from a common key, extension-converting a result obtained by substituting, with an S box, an exclusive OR of a constant set in accordance with the round number and a first key generated from the temporary key as a key conversion function, and calculating an extended key based on the result of the conversion and a second key generated from the temporary key. Thus, it is understood in particular that the three elements of the exclusive OR by the constant, nonlinear conversion with an S box and extension conversion are integrally used, so that the technical problem can be solved.

On the other hand, the present application neither discloses nor suggests a technique for inputting different keys in the respective rounds, performing a conversion process with a predetermined conversion table based on the first key obtained from the input key, and calculating an extended key based on the conversion result and a second key obtained from the input key. Therefore, it is unclear how the claimed invention achieves the object and effect described in the specification of the present application.

Thus, the invention recited in claims 1 to 26 is not described in the detailed description of the invention.

If a new reason for rejection is found, a further Notification of

Reasons for Rejection will be issued.

Prior Art Search Report

Searched Field: IPC 7th ed.

G09C1/00, H04L9/00

Prior Art Document:

Jpn. Pat. Appln. KOKAI Publication No. 11-338345

The document does not constitute the reason for rejection.

整理番号　Ａ０００００４７７６　　発送番号　１９４９３０
発送日　平成１４年　６月１８日　　

拒絶理由通知書

特許出願の番号	特願２０００－２６１０９８
起案日	平成１４年　６月１３日
特許庁審査官	青木　重徳　　４２２９　５Ｍ００
特許出願人代理人	鈴江　武彦（外　６名）　様
適用条文	第２９条柱書、第２９条第２項、第３６条

14.8.17

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から６０日以内に意見書を提出して下さい。

理　由

【Ａ】この出願の下記の請求項に係る発明は、下記の点で特許法第２９条第１項柱書に規定する要件を満たしていないので、特許を受けることができない。

記

・請　求　項：１１，２５
・備　　考
計算法、作図法と認められる発明は、一般に人間の推理力や記憶力を利用するものであって自然法則利用の技術的手段を伴うものでないから、特許法第２条に定義されている発明とは認められず、同法第２９条の特許要件を備えていないと解するのが原則である。
そして、請求項１１や請求項２５に記載されている「拡大鍵生成方法」は、一般的に数値表現として表される暗号鍵から計算や作図により拡大鍵を生成する方法を定義したものであり、その間何らの装置を伴っていないことを勘案すれば、上記原則を類推適用できる。
よって、請求項１１，２５に係る発明は特許法第２条でいう「発明」には該当しない。

・請　求　項：１２－２１，２６
・備　　考
請求項１２－２１，２６に記載されている「コンピュータ読取り可能な記憶媒体」は、その間何らの技術的手段を用いていないことから、単に人為的な取り決めを定義したプログラムを記憶しただけのものであるから、請求項１２－２１，２６に係る発明は情報の単なる提示に過ぎず、よって特許法第２条でいう「発明」には該当しない。

SS，松下

【Ｂ】この出願の下記の請求項に係る発明は、その出願前日本国内において頒布された下記の刊行物に記載された発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記　　（引用文献等については引用文献等一覧参照）

・請　求　項：１，４，５
・引用文献等：１
・備　　考

引用文献１には、カスケードに連結された中間鍵の生成回路からなる鍵スケジュール部を有し、前記各中間鍵の生成回路は、入力された鍵から得られた第１鍵に基づいて所定の所定の関数により変換処理を行い、この結果と入力された鍵から得られた第２鍵とに基づいて中間鍵を算出する装置が記載されている。

ところで、引用文献１に記載されているものでは、鍵の変換を関数処理により得ているが、該関数の処理はいわゆるｓボックスを用いた置換テーブルに基づくものであることを勘案すれば、引用文献１に記載されているものは、本願請求項１に係る発明と本質的に同様な機能構成を有するものである。

・請　求　項：２
・引用文献等：１，２
・備　　考

引用文献２には、入力された鍵を左シフトさせて次の鍵スケジュール部に入力する鍵スケジュール部が記載されている。

そして、引用文献１，２が共に拡大鍵の生成技術について記載したものである点を勘案すれば、引用文献１に記載されているものにおける次の鍵スケジュール部への入力構成として、引用文献２に記載されているのもを採用することは、当業者が容易になし得たことである。

・請　求　項：９，１０
・引用文献等：１
・備　　考

引用文献１に記載されているものでは、生成された複数の中間鍵を各ラウンド毎の関数処理の鍵として使用し、平文を暗号化し、暗号文を平文とする攪拌処理を行っている。

・請　求　項：１１，１２，２０，２１，２５，２６
・引用文献等：１
・備　　考

引用文献１には、カスケードに連結された中間鍵の生成回路からなる鍵スケジュール部を有し、前記各中間鍵の生成回路は、入力された鍵から得られた第１鍵に基づいて所定の所定の関数により変換処理を行い、この結果と入力された鍵から得られた第２鍵とに基づいて中間鍵を算出する方法が記載されている。

ところで、引用文献１に記載されているものでは、鍵の変換を関数処理により得ているが、該関数の処理はいわゆるｓボックスを用いた置換テーブルに基づくものであることを勘案すれば、引用文献１に記載されているものは、本願請求項１に係る発明と本質的に同様な機能を有するものであるし、このような方法をコンピュータで実現するためにプログラム化して記憶媒体に記録しておくことは、当業者にとって常套手段である。

・請　求　項：１３
・引用文献等：１，２
・備　　考

引用文献２には、入力された鍵を左シフトさせて次の鍵スケジュール部に入力する鍵スケジュール部が記載されている。

そして、引用文献１，２が共に拡大鍵の生成技術について記載したものである点を勘案すれば、引用文献１に記載されているものにおける次の鍵スケジュール部への入力として、引用文献２に記載されているのもを採用することは、当業者が容易になし得たことであるし、このような方法をコンピュータで実現するためにプログラム化して記憶媒体に記録しておくことは、当業者にとって常套手段である。

。

引　用　文　献　等　一　覧

１．清水明宏，宮口庄司，“高速データ暗号アルゴリズムＦＥＡＬ”，
電子情報通信学会論文誌　Ｄ，日本，社団法人電子情報通信学会，
１９８７年　７月２０日，Ｖｏｌ．Ｊ７０－Ｄ，Ｎｏ．７，
ｐｐ．１４１３－１４２３
２．特開平１０－１１６０２９号公報

【Ｃ】この出願は、特許請求の範囲の記載が下記の点で、特許法第３６条第６項第１号に規定する要件を満たしていない。

記

本願明細書及び図面には、共通鍵から生成された一時鍵を入力し、鍵変換関数としてラウンド数に対応して設定された定数を前記一時鍵から生成した第１鍵と排他的論理和した結果をＳボックスによって置換したものを拡大変換し、その結果と前記一時鍵から生成した第２鍵とに基づいて拡大鍵を算出する技術が記載さ

れており、特に定数による排他的論理和、Ｓボックスによる非線形変換、拡大変換という３つの構成要素を一体で用いることにより技術課題の解決を図っていることが理解できる。

これに対し、本願発明は、各ラウンド毎に異なる鍵が入力され、この入力された鍵から得られた第１鍵に基づいて所定の置換テーブルにより変換処理を行い、この変換結果と入力された鍵から得られた第２鍵とに基づいて拡大鍵を算出する技術は開示も示唆もされておらず、請求項　に係る発明が本願明細書に記載されている目的、効果をどのように達成するのか不明である。。

よって、請求項１－２６に係る発明は、発明の詳細な説明に記載したものでない。

拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

先行技術文献調査結果の記録

・調査した分野　　ＩＰＣ第７版
　Ｇ０９Ｃ１／００，Ｈ０４Ｌ９／００
・先行技術文献
　特開平１１－３３８３４５号公報

この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。